PATENT SPECIFICATION (11) 1 582 989

1 582 989

(21) Application No. 48706/77 (22) Filed 23 Nov. 1977

(23) Complete Specification filed 26 May 1978

(44) Complete Specification published 21 Jan. 1981

(51) INT. CL.³ G06K 19/00

(52) Index at acceptance
G4M A1 A2 C1 F10 F3 F4 FX K1 RX WX WY

(72) Inventor BRIAN FREELAND WILKIE

(19)

(54) IMPROVEMENTS IN SECURITY SYSTEMS

(71) We, MOTOROLA, INC., a corporation organised and existing under the laws of the State of Delaware, United States of America, of Motorola Center, 1303 East Algonquin Road, Schaumburg, Illinois 60196, United States of America, do hereby declare the invention, for which we pray that a patent may be granted to us, and the method by which it is to be performed, to be particularly described in and by the following statement:–

This invention relates to security systems and particularly to a security device known as a key card.

In recent years the conventional mechanical key has been replaced in many security systems by an electronic or electromechanical device which enables authorised personnel to gain access through doors, operate machinery and other equipment such as cash dispensers and the like. Such devices are known as, and will be referred to hereinafter as 'key cards'.

Known key cards generally comprise a sheet of durable plastics material which is provided with some form of permanent or non-volatile memory, such as physical holes or cut outs or magnetic strips, containing data which when presented to an electromechanical reader either performs a desired function or does not depending on the instructions programmed into the reader. In its simplest form the reader can be programmed with an "entry permitted" code which it compares with a code in the non-volatile memory of the key card and if codes are identical the reader operates a mechanical device to open the relevant door or the like. Until now all such known key cards have been provided with permanent or non-volatile memories. A non-volatile memory is one which is capable of retaining its data in the absence of any power source. A permanent memory is one which cannot have the data contained removed and replaced with different data, for example, a punch card.

The aforementioned key cards suffer from a number of disadvantages in that their stored information can be read by unauthorised personnel and with the correct equipment the data can be decoded and consequently duplicated. Moreover, such known key cards do not lend themselves to regular modification of the stored data, for example, on a weekly basis.

An object of the present invention is to obviate or mitigate the above disadvantages.

According to one aspect of the present invention there is provided a security key card having a volatile memory for the receipt and storage of data.

According to a further aspect of the present invention there is provided a security system comprising a security lock and a security key card provided with a volatile memory device, the security key card being arranged in cooperative relationship such that when the key card is presented to the lock two-way communication of data is effected.

The invention will now be described by way of example only with particular reference to the accompanying drawings, in which:–

Fig. 1 is a block circuit diagram of a security key card in accordance with a first embodiment of the invention and

Fig. 2 is a block circuit diagram of a security key card in accordance with a second embodiment of the invention.

A block diagram of a key card for an electronic "lock" (not shown) which will enable access through a door is shown in Fig. 1 and comprises a connector terminal block 1 having eight terminals A to H, one of which viz. C establishes a path C' for electrical signals to pass in both directions between a lock and the key card and the remaining terminals establishing paths A', B', D', E', F', G' for electrical signals to pass unidirectionally from the lock to the key card and from the key card to the lock for path H'. Path C' is the 'data-bus' which carries binary data to and from a Control Unit indicated at 2. The control unit 2 is a silicon integrated circuit such as that sold as internationally classified electronic part No. MC 14500B and forms the intelligent heart of the key card manipulating information on the data bus C in

accordance with instructions stored in a Random Access Memory (RAM) shown at 3 in Fig. 1 and comprising a silicon integrated circuit of the type classified as MCM14552. The RAM consists of a number of storage locations, in this case sixty-four, each of which contains four binary bits. These four bit programme words are interpreted by the control unit 2 as one of sixteen operations to be carried out on the data bus C'.

The RAM 3 presents the programme words, sequentially, one at a time to the control unit 2 under the control of a programme counter 4 comprising an integrated circuit such as part MC 14520 and which steps the system sequentially from one programme word to the next. The control unit 2 has the ability to make decisions based on the state of the data bus C' and to reset the counter 4 to its "start position", via line 6 connected to reset path B'. Reset can also be achieved in response to a signal supplied by the lock along reset path B' and a clock path A' is also provided along which a signal may pass from the lock so as to instruct the counter 4 to advance to the next step in the key card's programme. The paths A' and B' thus serve to synchronise the operations of the lock and kay card. The 'clock' timing signals and the reset signals are also supplied respectively to the control unit on lines A", B".

Paths D', E', F' and G' and their associated connectors are provided to allow the lock to pass new programme words directly to the RAM 3, the paths being such as to allow data to pass in that one direction only. An energy source 5 is connected to the counter 4, the memory 3 and control unit 2 to provide the power for the integrated circuits thereof and is utilised both when the key card is connected to the lock and also to retain the information stored in the memory as the latter is volatile and will therefore lose the data if the power source is disconnected. The key card is constructed in a manner such that dismantling thereof cannot proceed without first disconnecting the energy source, the latter being a battery or a charged capacitor. Since the memory retention depends on a constant supply of energy from the source 5 any attempt to tamper with the key card will erase the memory.

The operation of the security system is as follows. A person holding a key card inserts the connector in the lock, this being the sole mechanical component of the system. The lock then sends a pulse on the reset path B' to ensure that the key card starts at the beginning of its programme. The lock then sends a short pattern of binary data along the data bus C' each accompanied by a pulse along the clock path A' to advance the counter 4 to the next location in the RAM 3. This initial pattern serves to establish the correct operation of the control unit 2 and any mistake in the pattern will cause all further data to be ignored.

The lock is now programmed to send a further string of binary signals along the data bus C'. If and only if this pattern is identical to that stored in the RAM 3 can the next stage proceed. Failing such a match the control unit 2 will reset itself and check for another match. The data which might typically consist of 10 pulses, giving a total of 1024 possible codes serves as a 'signature' for the lock and without first receiving the correct 'signature' the key card will not output any data. At this stage assuming a match has been made the key card will send a string of binary data along the data bus C' to the lock so as to identify the person presenting the card and to pass to the lock any other relevant information. As an additional safeguard this code can be modified in accordance with instructions from the lock for use on the next occasion. The data string may be as long as thirty "ones" and "zeros" giving a large number of possible codes. If the code supplied by the key card is acceptable to the lock then access will be permitted to the key card holder by the lock opening.

In a second embodiment of the invention shown in Fig. 2, the connector is shown at 7 and includes paths J' to R'. As before a control unit is provided at 8 but in this case the memory is provided by a pair of shift registers 9*a*, 9*b*; which memorise sixty-four – four bit words. This is achieved using two integrated circuits of the type MC 14517 B and an associated multiplexer 10 of the type MC 14519 B, the latter allowing data retention under normal operation as well as the insertion of new programme words. Such a memory has the same power dependent retention property as the RAM but cannot be reset during a cycle. This requires a change in the operating system such that on detection of an erroneous lock signature code the output is disabled for the rest of the cycle. Moreover, the synchronisation of the key card and the lock must be controlled in this embodiment by a signal from the key card at the start of each cycle. Otherwise the operation is similar with the power source at 11, and O' being the unidirectional clock signal path, P' being the two-way data path, Q' the synchronising signal path, N' the multiplex control path J' to M' the new programme paths. In the second embodiment R' is the signal return path.

With the system of the invention the lock and key card are not limited to a single code combination. In fact by merely applying the correct signals to the connector 1 (Figure 1) and 7 (Figure 2) the key card may be recoded and can incorporate a change of

operating procedure. Furthermore, it will be realised that the invention envisages key cards only valid at certain times or for a limited period of time and by allowing the locks to manipulate the programme once pass words have been successfully exchanged the key card could store other information such as the number of journeys travelled using a season ticket type key card. In this case the key card would be charged with say twenty-five journeys in code from each time payment is made at the ticket office. Each use of the key card thereafter in a ticket barrier would decrement the allowable journey total until zero was reached. As a further extension of this principle the key card can be used as a credit card. The owner's bank balance can be stored in the card and automatically recalculated as each purchase is made without the necessity of the "lock" being connected to a central computer complet.

WHAT WE CLAIM IS:

1. A security key card having a volatile memory device for the receipt and storage of data.

2. A security key card as claimed in claim 1 including terminal means having a plurality of terminals to establish unidirectional electrical signal paths for the passage of electrical signals from a security lock device and the key card and at least one terminal serving to establish a bi-directional path for the passage of data in both directions between the volatile memory device and the lock.

3. A security key card as claimed in claim 1 or 2 wherein the volatile memory device is a random access memory device.

4. A security key card as claimed in claim 2 or 3 wherein said memory device has outputs thereof connected to corresponding inputs of a control unit connected to the bi-directional path in accordance with programme data stored in storage locations of the memory device.

5. A security key card as claimed in claim 4 wherein data is presented sequentially to the control unit from the memory device under the control of a programme counter connected to the memory device whereby the control unit effects decisions based on the data present in the bi-directional path.

6. A security key card as claimed in claim 5 wherein one of said unidirectional paths is connected to one input of the programme counter and is supplied with timing signals from the lock to advance the counter to the next step in the programme, a second input of the counter being connected to a further unidirectional path to effect reset of the counter in response to a reset signal from the lock and to synchronise the operation of the lock and key card, and said control unit having an output thereof connected to said reset path to allow the control unit to reset the programme counter.

7. A security key card as claimed in any of claims 2 to 6 wherein a selected number of said plurality of unidirectional paths are connected to corresponding inputs of the memory device, to allow programme data to pass directly from the lock to the memory device and a further unidirectional path is connected to a source of energy which is connected to inputs of the programme counter, memory device and control unit to supply power thereto and to pass a return signal to the lock along said further unidirectional path.

8. A security key card as claimed in claim 5 wherein the volatile memory device comprises shift register means, multiplexer means having a selected number of the unidirectional paths connected thereto and said multiplexer means also being connected to inputs of the shift register means to allow data retention in the memory device under normal operation of the key card and to allow programme data to be introduced into the memory device, and means for disabling the key card if during a cycle of the programme counter, the data stored in the memory device does not correspond with data in the bi-directional path received from the lock, and means for synchronising the key card and lock by supplying a signal from the key card to the lock via one of said unidirectional paths at the beginning of each cycle.

9. A security system comprising a security lock and a security key card provided with a volatile memory device, the security key card being arranged in cooperative relationship with the lock such that when the key card is presented to the lock, two-way communication of data is effected.

10. A security system as claimed in claim 9 wherein the key card includes terminal means having a plurality of terminals to establish a plurality of unidirectional paths for the passage of data signals between the card and the lock, at least one bi-directional path for the passage of data signals in both directions between the card and the lock, a control unit connected to said bi-directional path, and to said memory device to receive programme signals therefrom, programme counter means having outputs connected to corresponding inputs of the memory device to control the transfer of data therefrom to the control unit, timing means to supply timing signals from the lock to the programme counter and control unit, means for supplying programme data over a plurality of said unidirectional paths from the lock to the memory device, means for comparing the data stored in the memory device with data supplied to the control unit over said bi-directional path to obtain a 'sig-

nature' for the lock and to allow data to be sent from the key card to the lock in response to said 'signature' to effect opening of the lock.

11. A system as claimed in claim 10 including means for inhibiting the output of data from the key card when an erroneous 'signature' is obtained.

12. A system as claimed in claim 10 or 11 including means for synchronising the key card and lock at the beginning of each cycle.

13. A security key card substantially as hereinbefore described and as shown in the accompanying drawings.

For the Applicants:
F. J. CLEVELAND & COMPANY,
Chartered Patent Agents,
40/43 Chancery Lane,
London, WC2A 1JQ.

Printed for Her Majesty's Stationery Office by The Tweeddale Press Ltd., Berwick-upon-Tweed, 1980. Published at the Patent Office, 25 Southampton Buildings, London, WC2A 1AY, from which copies may be obtained.

1582989 COMPLETE SPECIFICATION

2 SHEETS *This drawing is a reproduction of the Original on a reduced scale*

Sheet 1

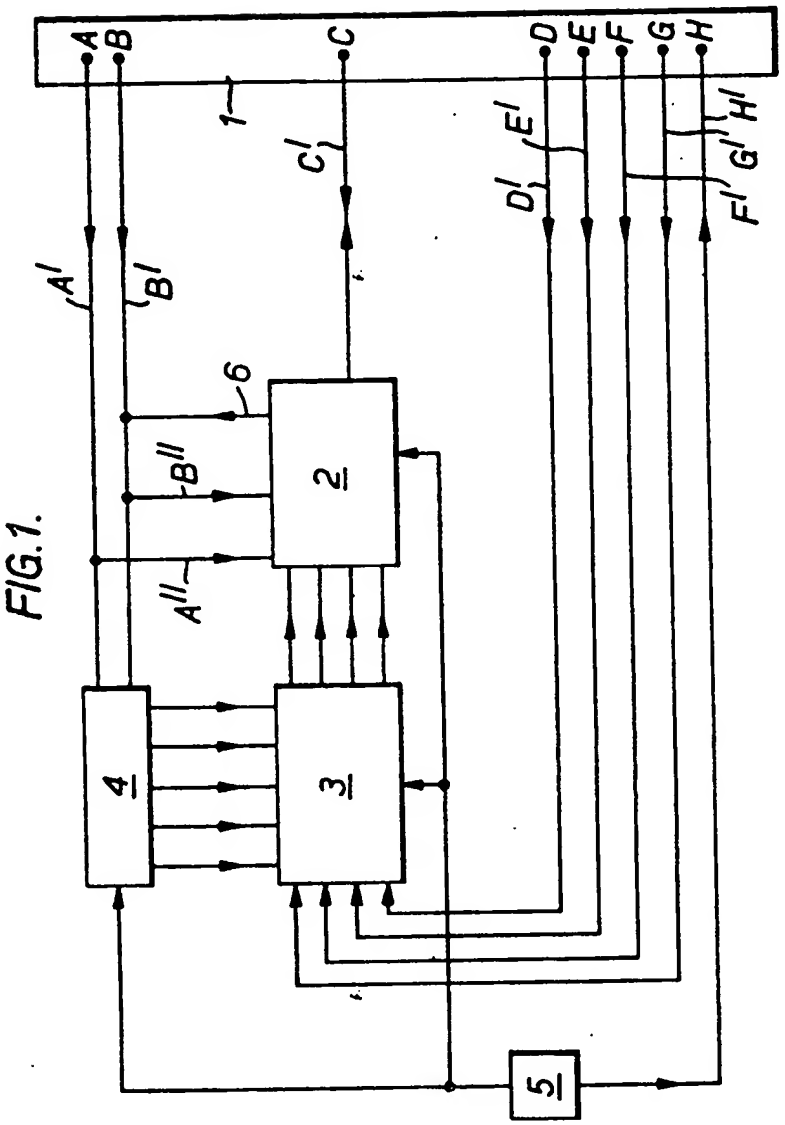

FIG.1.

1582989 COMPLETE SPECIFICATION

2 SHEETS *This drawing is a reproduction of the Original on a reduced scale*

Sheet 2

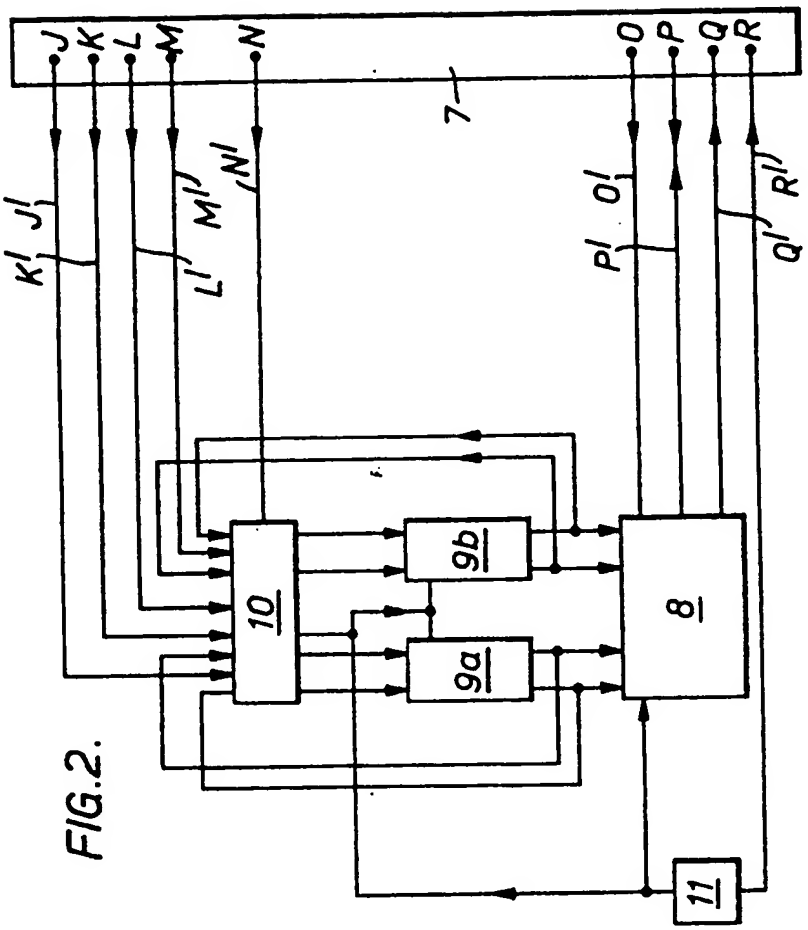

FIG.2.